# Inherently Safer Design and Chemical Plant Security and Safety

Prepared for submission to the
United States House of Representatives Homeland Security Committee
June 29, 2006
Washington, DC


Scott Berger
Director
Center for Chemical Process Safety
American Institute of Chemical Engineers
3 Park Avenue
New York, NY 10016
(212) 591-7237
Fax (212) 591-8883
scotb@aiche.org
http://www.aiche.org/ccps

Dennis C. Hendershot
Staff Consultant
Center for Chemical Process Safety
American Institute of Chemical Engineers
534 Norris Drive
Furlong, PA 18925
(215) 345-0760
Fax (215) 489-9250 (call first)
dchendershot@member.aiche.org
http://home.att.net/~d.c.hendershot/

Karen Person
Project Engineer
Center for Chemical Process Safety
American Institute of Chemical Engineers
3 Park Avenue
New York, NY 10016
(212) 591-7319
Fax (212) 591-8883
karep@aiche.org
http://www.aiche.org/ccps


The Center for Chemical Process Safety (CCPS) is sponsored by the American Institute of Chemical Engineers (AIChE), which represents Chemical Engineering Professionals in technical matters in the United States. CCPS is dedicated to eliminating major incidents in chemical, petroleum, and related facilities by:

- Advancing state of the art process safety technology and management practices
- Serving as the premier resource for information on process safety
- Fostering process safety in engineering and science education
- Promoting process safety as a key industry value

CCPS was formed by AIChE in 1985 as the chemical engineering profession's response to the Bhopal, India chemical release tragedy. In the past 21 years, CCPS has defined the basic practices of process safety and supplemented this with a wide range of technologies, tools, guidelines, and informational texts and conferences. CCPS' output includes more than 70 Guideline books, more than 90 university lectures, and a monthly e-mail process safety lesson delivered to more than 600,000 plant personnel around the world in 17 languages. The CCPS book "Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites" (2002) has been used by thousands of plants around the world to evaluate chemical facility security, and is the basis for New Jersey State security regulation and the voluntary security programs of numerous chemical and petroleum trade associations. Today, CCPS has more than 85 member companies in the US and around the world, and maintains an active program to continue advancing the practice of process safety.

CCPS supports national legislation addressing the security of facilities that manufacture and use chemicals. The House Bill as it exists today addresses all the important points that CCPS believes are critical to chemical security. It has been suggested that the Bill should also address the use of Inherently Safer Technologies. As the organization that developed the most widely-used reference addressing Inherently Safer Design ("Inherently Safer Processes: A Lifecycle Approach", AIChE Press, New York, 1996), we wanted to take this opportunity to explain the fundamentals of Inherently Safer Design, the challenges and trade-offs, and the limitations relative to security

**<u>What is inherently safer design?</u>**

Inherently safer design is a concept related to the design and operation of chemical plants, and the philosophy is generally applicable to any technology. Inherently safer design is not a specific technology or set of tools and activities at this point in its development. It continues to evolve, and specific tools and techniques for application of inherently safer design are in early stages of development. The CCPS book, and other literature on inherently safer design (for example, by CCPS, Trevor Kletz, and others) describe a design philosophy and give examples of implementation, but do not describe a methodology. CCPS has begun a project to update its 1996 book on inherently safer design, and one of the objectives for this second edition is to propose one or more specific methods for implementation. These methods will hopefully be confirmed and expanded upon with use, so that at some time in the future more robust methods will exist. Such methods do not exist now.

What do we mean by inherently safer design? One dictionary definition of "inherent" which fits the concept very well is "existing in something as a permanent and inseparable element." This means that safety features are built into the process, not added on. Hazards are eliminated or significantly reduced rather than controlled and managed. The means by which the hazards are eliminated or reduced are so fundamental to the design of the process that they cannot be changed or defeated without changing the process. In many cases this will result in simpler and cheaper plants, because the extensive safety systems which may be required to control major hazards will introduce cost and complexity to a plant. The cost includes both the initial investment for safety equipment, as well as the ongoing operating cost for maintenance and operation of safety systems throughout the life of the plant.

Chemical process safety strategies can be grouped in four categories:

- Inherent – as described in the previous paragraphs (for example, replacement of an oil based paint in a combustible solvent with a latex paint in a water carrier)
- Passive – safety features which do not require action by any device, they perform their intended function simply because they exist (for example, a blast resistant concrete bunker for an explosives plant)
- Active – safety shutdown systems to prevent accidents (for example, a high pressure switch which shuts down a reactor) or to mitigate the effects of accidents (for example, a sprinkler system to extinguish a fire in a building). Active systems require detection of a hazardous condition and some kind of action to prevent or mitigate the accident.

- Procedural – Operating procedures, operator response to alarms, emergency response procedures

In general, inherent and passive strategies are the most robust and reliable, but elements of all strategies will be required for a comprehensive process safety management program when all hazards of a process and plant are considered.

Approaches to inherently safer design fall into these categories:

- Minimize – significantly reduce the quantity of hazardous material or energy in the system, or eliminate the hazard entirely if possible
- Substitute – replace a hazardous material with a less hazardous substance, or a hazardous chemistry with a less hazardous chemistry
- Moderate – reduce the hazards of a process by handling materials in a less hazardous form, or under less hazardous conditions, for example at lower temperatures and pressures
- Simplify – eliminate unnecessary complexity to make plants more "user friendly" and less prone to human error and incorrect operation

One important issue in the development of inherently safer chemical technologies is that the property of a material which makes it hazardous may be the same as the property which makes it useful. For example, gasoline is flammable, a well known hazard, but that flammability is also why gasoline is useful as a transportation fuel. Gasoline is a way to store a large amount of energy in a small quantity of material, so it is an efficient way of storing energy to operate a vehicle. As long as we use large amounts of gasoline for fuel, there will have to be large inventories of gasoline somewhere.

## Inherently safer design and the chemical industry

While some people have criticized the chemical industry for resisting inherently safer design, we believe that history shows quite the opposite. The concept of inherently safer design was first proposed by an industrial chemist (Trevor Kletz, of ICI in the UK), and it has been publicized and promoted by many technologists from petrochemical and chemical companies – ICI, Dow, Rohm and Haas, ExxonMobil, and many others. The companies that these people work for have strongly supported efforts to promote the concept of inherently safer chemical technologies.

The members of CCPS enthusiastically supported the publication of the Inherently Safer Processes book in 1996. Several companies ordered large numbers of copies of the book for distribution to their chemists and chemical engineers. CCPS members have recognized a need to update this book after 10 years, and there is a current project to write a second edition of the book, with active participation by CCPS member companies.

There has been some isolated academic activity on how to measure the inherent safety of a technology (and no consensus on how to do this), but we have seen little or no academic research on how to actually go about inventing inherently safer technology. All of the papers and publications that we have seen describing inherently safer technologies have either been written by people working for industry, or describe designs and technologies developed by industrial companies. And, we suspect that there are many more examples which have not been described. We believe that industry has strongly advocated inherently safer design, supporting the writing of CCPS books on the subject, teaching the concept to engineers (who most likely never heard of it during their college education), and incorporating it into internal process safety management programs. Nobody wants to spend time, money, and scarce technical resources managing hazards if there are viable alternatives that make this unnecessary.

**Inherently safer design and security**

Safety and security are good business. Safety and security incidents threaten a community's willingness to allow a plant to operate in their neighborhood, while good performance in these areas results in an improved community image for the company and plant, reduced risk and actual losses, and increased productivity, as discussed in the CCPS publication, "Business Case for Process Safety," which has been recently revised and updated.

A terrorist attack on a chemical plant that causes a toxic release can have the same kinds of potential consequences as accidental events resulting in loss of containment of a hazardous material or large amounts of energy from a plant. Clearly anything which reduces the amount of material, the hazard of the material, or the energy contained in the plant will also reduce the magnitude of this kind of potential security related event. The chemical industry recognizes this, and current security vulnerability analysis protocols require evaluation of the magnitude of consequences from a possible security related loss of containment, and encourage searching for feasible means of reducing these consequences. But inherently safer design is not a solution which will resolve all issues related to chemical plant security. It is one of the tools available to address concerns, and needs to be used in conjunction with other approaches, particularly when considering all potential security hazards.

In fact, inherently safer design will rarely avoid the need for implementing conventional security measures. To understand this, one must consider the four main elements of concern for security vulnerability in the chemical industry:

- Off-site consequences from toxic release, a fire, or an explosion
- Theft of material or diversion to other purposes, for example the ammonium nitrate used in the first attempt to destroy the World Trade Center in New York, or for the Oklahoma City bombing
- Contamination of products, particularly those destined for human consumption such as pharmaceuticals, food products, or drinking water
- Degradation of infrastructure such as the loss of communication ability from the second World Trade Center attacks

Inherently safer design of a process addresses the first bullet, but does not have any impact whatsoever on conventional security needs for the others. A company will still need to protect the site the same way, whether it uses inherently safer processes or not. Therefore, inherently safer design will not significantly reduce security requirements for a plant.

The objectives of process safety management and security vulnerability management in a chemical plant are safety and security, not necessarily inherent safety and inherent security. It is possible to have a safe and secure facility for a facility with inherent hazards. In fact this is essential for a facility for which there is no technologically feasible alternative – for example, we cannot envision any way of eliminating large inventories of flammable transportation fuels in the foreseeable future.

An example from another technology – one which many of us frequently use – may illustrate how the true objective of safety and security management is safety and security, not inherent safety and security. Airplanes have many major hazards associated with their operation, and we have seen airplanes used for terrorism. In fact, essentially the entire population of the United States, or even the world, is potentially vulnerable to this hazard.

Airlines are in the business of transporting people and things from one place to another. They are not really in the business of flying airplanes – that is just the technology they have selected to accomplish their real business purpose. Inherently safer technologies which completely eliminate this hazard are available – high speed rail transport is well developed in Europe and Japan.

But we do not require airline companies to adopt this technology, or even to consider it and justify why they do not adopt it. We recognize that the true objective is "safety" and "security" not "inherent safety" or "inherent security." The passive, active, and procedural risk management features of the air transport system have resulted in an enviable, if not perfect, safety record, and nearly all of us are willing to travel in an airplane or allow them to fly over our homes.

**<u>Some issues and challenges in implementation of inherently safer design</u>**

- The chemical industry is a vast interconnected ecology of great complexity. There are dependencies throughout the system, and any change will have cascading effects throughout the chemical ecosystem. It is possible that making a change in technology that appears to be inherently safer locally at some point within this complex enterprise will actually increase hazards elsewhere once the entire system reaches a new equilibrium state. Such changes need to be carefully and thoughtfully evaluated to fully understand all of their implications.
- In many cases it will not be clear which of several potential technologies is really inherently safer, and there may be strong disagreements about this. Chemical processes and plants have multiple hazards, and different technologies will have different inherent safety characteristics with respect to each of those multiple hazards. Some examples of chemical substitutions which were thought to

be safer when initially made, but were later found to introduce new hazards include:

  - Chlorofluorcarbon (CFC) refrigerants – low acute toxicity, non-flammable, but later found to have long term environmental impacts
  - PCB transformer fluids – non-flammable, but later determine to have serious toxicity and long term environmental impacts

- Who is to determine which alternative is inherently safer, and how to make this determination? This decision requires consideration of the relative importance of different hazards, and there may not be agreement on this relative importance. This is particularly a problem with requiring the implementation of inherently safer technology – who determines what that technology is? There are tens of thousands of chemical products manufactured, most of them by unique and specialized processes. The real experts on these technologies, and on the hazards associated with the technology, are the people who invent the processes and run the plants. In many cases they have spent entire careers understanding the chemistry, hazards, and processes. They are in the best position to understand the best choices, rather than a regulator or bureaucrat with, at best, a passing knowledge of the technology. But, these chemists and engineers must understand the concept of inherently safer design, and its potential benefits – we need to educate those who are in the best position to invent and promote inherently safer alternatives.
- Development of new chemical technology is not easy, particularly if you want to fully understand all of the potential implications of large scale implementation of that technology. History is full of examples of changes that were made with good intentions that gave rise to serious issues which were not anticipated at the time of the change, such as the use of CFCs and PCBs mentioned above. Co-author Hendershot personally has published brief descriptions of an inherently safer design for a reactor in which a large batch reactor was replaced with a much smaller continuous reactor. This is easy to describe in a few paragraphs, but actually this change represents the results of several years of process research by a team of several chemists and engineers, followed by another year and millions of dollars to build the new plant, and get it to operate reliably. And, the design only applies to that particular product. Some of the knowledge might transfer to similar products, but an extensive research effort would still be required. Furthermore, Dennis Hendershot has also co-authored a paper which shows that the small reactor can be considered to be less inherently safe from the viewpoint of process dynamics – how the plant responds to changes in external conditions – for example, loss of power to a material feed pump. The point – these are not easy decisions and they require an intimate knowledge of the process.
- Extrapolate the example in the preceding paragraph to thousands of chemical technologies, which can be operated safely and securely using an appropriate blend of inherent, passive, active, and procedural strategies, and ask if this is an appropriate use of our national resources. Perhaps money for investment is a lesser concern – do we have enough engineers and chemists to be able to do

this in any reasonable time frame? Do the inherently safer technologies for which they will be searching even exist?

- The answer to the question "which technology is inherently safer?" may not always the same – there is most likely not a single "best technology" for all situations. Consider this non-chemical example. Falling down the steps is a serious hazard in a house and causes many injuries. These injuries could be avoided by mandating inherently safer houses – we could require that all new houses be built with only one floor, and we could even mandate replacement of all existing multi-story houses. But would this be the best thing for everybody, even if we determined that it was worth the cost? Many people in New Orleans survived the flooding in the wake of Hurricane Katrina by fleeing to the upper floors or attics of their houses. Some were reportedly trapped there, but many were able to escape the flood waters in this way. So, single story houses are inherently safer with respect to falling down the steps, but multi story houses may be inherently safer for flood prone regions. We need to recognize that decision makers must be able to account for local conditions and concerns in their decision process.
- Some technology choices which are inherently safer locally may actually result in an increased hazard when considered more globally. A plant can enhance the inherent safety of its operation by replacing a large storage tank with a smaller one, but the result might be that shipments of the material need to be received by a large number of truck shipments instead of a smaller number of rail car shipments. Has safety really been enhanced, or has the risk been transferred from the plant site to the transportation system, where it might even be larger?
- We have a fear that regulations requiring implementation of inherently safer technology will make this a "one time and done" decision. You get through the technology selection and pick the inherently safer option, meet the regulation, and then you don't have to think about it any more. We want engineers to be thinking about opportunities for implementation of inherently safer designs at all times in everything they do – it should be a way of life for those designing and operating chemical, and other, technologies. For example:
    - Research chemists and engineers – inherently safer fundamental chemistries
    - Process development engineers – inherently safer processes based on those chemistries
    - Design engineers – inherently safer plant design using the selected technology and process
    - Detailed design engineers – inherently safer equipment details – minimize the length and size of pipes, vessels, and other equipment, make the plant design "user friendly"
    - Plant operation engineers and operators – develop inherently safer operating procedures, look for opportunities for enhancing inherent safety in existing facilities
    - Operators – look for inherently safer ways to do all of the tasks involved in the day to day operation of a plant

Inherently safer design and operation needs to be the way everybody involved in chemical technology thinks, not just a one time exercise to comply with a regulation.

- Inherently safer processes require innovation and creativity. How do you legislate a requirement to be creative? Inherently safer alternatives can not be invented by legislation.

**<u>What should we be doing to encourage inherently safer technology?</u>**

Inherently safer design is primarily an environmental and process safety measure, and its potential benefits and concerns are better discussed in context of future environmental legislation, with full consideration of the concerns and issues discussed above. While consideration of inherently safer processes does have value in some areas of chemical plant security vulnerability – the concern about off site impact of releases of toxic materials – there are other approaches which can also effectively address these concerns, and industry needs to be able to utilize all of the tools in determining the appropriate security vulnerability strategy for a specific plant site. Some of the current proposals regarding inherently safer design in security regulations seem to drive plants to create significant paperwork to justify not using inherently safer approaches, and this does not improve security.

We believe that future invention and implementation of inherently safer technologies, to address both safety and security concerns, is best promoted by enhancing awareness and understanding of the concepts by everybody associated with the chemical enterprise. They should be applying this design philosophy in everything they do, from basic research through process development, plant design, and plant operation. Also, business management and corporate executives need to be aware of the philosophy, and its potential benefits to their operations, so they will encourage their organization to look for opportunities where implementing inherently safer technology makes sense.

We believe that the approach that the Environmental Protection Agency has taken to promote Green Chemistry provides a good example of how the Federal government can promote the adoption of inherently safer technology in industry. EPA has been active in promoting the principals of green chemistry, promoting incorporation of green chemistry into the education of chemists, and in sponsoring conferences and technical meetings on the subject. Each year a number of awards are given to researchers and to companies for outstanding examples of implementation of green chemistry. An effort like this for inherently safer design will increase its visibility for all chemical industry technologists, promote sharing of ideas and information, recognize important contributions, and encourage others to understand and apply the principles of inherently safer design.